



DEPARTMENT OF HOMELAND SECURITY

[Docket No. ICEB-2020-0009]

Privacy Act of 1974; System of Records

AGENCY: U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security.

ACTION: Notice of Modified Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the U.S. Department of Homeland Security (DHS) proposes to modify, rename, and reissue a current U.S. Immigration and Customs Enforcement (ICE) system of records titled, “DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS) System of Records.” DHS/ICE uses, collects, and maintains information on nonimmigrant students and exchange visitors, and their dependents, admitted to the United States under an F, M, or J class of admission, and the schools and exchange visitor program sponsors that host these individuals in the United States. DHS/ICE is updating the name of this system of records; modifying existing and adding new categories of individuals and categories of records; and updating, modifying, and removing routine uses. Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act, elsewhere in the *Federal Register*. This updated system of records will be included in DHS’s inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This modified system of records will be effective upon publication. New or modified routine uses will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number ICEB-2020-0009, by one of the following methods:

- Federal e-Rulemaking Portal: <https://www.regulations.gov/>. Follow the instructions for submitting comments.
- Fax: (202) 343-4010
- Mail: Lynn Parker Dupree, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number ICEB-2020-0009. All comments received will be posted without change to <https://www.regulations.gov/>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to <https://www.regulations.gov/>.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Jordan Holz, (202) 732-3300, Privacy Officer, ICEPrivacy@dhs.gov, U.S. Immigration and Customs Enforcement, 500 12th Street SW Stop 5004, Washington, D.C. 20536-5004. For privacy questions, please contact Lynn Parker Dupree, (202) 343-1717, Chief Privacy Officer, Privacy@hq.dhs.gov, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. sec. 552a, the U.S. Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) is updating, renaming, and reissuing a DHS system of records now titled, “DHS/ICE-001 Student and Visitor Exchange Program (SEVP)” System of Records.

The DHS/ICE update to SEVIS, now SEVP, includes several changes. First, the system of records is being renamed to better align it with the purpose of the system. This

system of records covers records on nonimmigrant students and exchange visitors, and their dependents, admitted to the United States under F, M, or J class of admission (hereinafter, “F/M/J nonimmigrants”), and the schools, designated program sponsors and host families that sponsor these individuals in the United States to ensure compliance with immigration laws and regulations and ensure their status is maintained. The SEVP coordinates with the Department of State (DOS), which oversees the operation of the U.S. Government’s Exchange Visitor (EV) Program, including the designation of EV Program sponsors, and supports the application and admission of foreign nationals who seek entry into the United States as exchange visitors (e.g., research scholar, government visitor, au pair) under the J class of admission.

In addition, the SEVP oversees the certification of academic and vocational schools to authorize enrollment of F and M nonimmigrant students based on federal regulations, and provides guidance and training to school officials about the SEVP certification requirements to which schools must adhere to and the requirements that their nonimmigrant students must follow to maintain their status.

Second, this update seeks to clarify and better identify the types of individuals and entities contained in this expanded system of records. Some items in the categories of individuals section have been reorganized and edited to more clearly identify the individuals, as well as expanded to include new categories of individuals, such as employers, financial support providers, government bodies and personnel, host families, members of the public, school employees, school partners, and school and EV Program officials.

Third, DHS/ICE has modified and expanded the categories of records section to better identify the types of information contained in the system of records. The new categories of records include education, employment, financial, travel, immigration-related information, school, program sponsor, case-related information, auditing and

training, reporting, and inquiries and data corrections.

Fourth, DHS/ICE is modifying Routine Use E and adding Routine Use F to conform to Office of Management and Budget (OMB) Memorandum M-17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information” (Jan. 3, 2017). All following routine uses are being re-lettered to account for the additional routine uses.

Finally, DHS is proposing to eliminate several routine uses, modify several routine uses, and add two new routine uses that would allow ICE to share information from the SEVP system of records with the specified recipients for the specified purpose. Below is a summary of those routine uses and their corresponding letter.

(J) Routine Use J is being updated to include disclosures to parties to an administrative proceeding where DHS has an interest in the outcome. This modification eliminates the need for two routine uses previously identified as Routine Uses K and L, and subsequent routine uses are being re-lettered to account for this change.

(O) Existing Routine Use P is being updated and re-lettered as Routine Use O to clarify that information may be shared about nonimmigrants between certified schools or programs as part of the transfer process from one school or program to another.

(R) Existing Routine Use S is being updated to be consistent with the DHS standard routine use for technology and is now Routine Use R. The modification eliminates the need for one routine use previously identified as Routine Use T, and subsequent routine uses are being re-lettered to account for this change.

(V) Routine Use V is being added to permit sharing identifying information with accrediting agencies, recognized by the Department of Education (ED), to facilitate the inspection and validation of schools and exchange visitor programs

in adherence to laws and regulations, and subsequent routine uses are being re-lettered to account for this additional routine use.

(W) Routine Use W is being added to clarify the sharing and disclosure of information to federal, state, local, and other government and public agencies, including foreign or international agencies when the information is relevant and necessary to DHS or a requesting agency's decision concerning the hiring or retention of an individual, or the issuance, grant, renewal, suspension or revocation of a security clearance, license, contract, grant or other benefit.

Information in the SEVP system of records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/ICE may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this SORN.

Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in the Federal Register. This modified system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies Fair Information Practice Principles in a statutory framework that governs the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A system of records is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other matched identifiers assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Further, those persons who do not currently fall under the

definition of individuals may naturalize or adjust status, thus becoming Privacy Act-covered individuals, over the course of this system's records retention schedule.

Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. The JRA also prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act. Below is the description of the DHS/ICE-001 Student and Exchange and Visitor Program (SEVP) system of records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the OMB and to Congress.

SYSTEM NAME AND NUMBER: U.S. Department of Homeland Security (DHS)/U.S. Immigration and Customs Enforcement (ICE)-001 Student and Exchange Visitor Program (SEVP).

SECURITY CLASSIFICATION: Unclassified, Controlled Unclassified Information. The data may be retained on classified networks, but this does not change the nature and character of the data until it is combined with classified information.

SYSTEM LOCATION: Records are maintained at the ICE Headquarters in Washington, D.C., and field offices. Records from SEVP systems may also be maintained in DHS unclassified and classified networks.

SYSTEM MANAGER(S): Systems Management Unit Chief, ICE Student and Exchange Visitor Program, 500 12th St. SW, MS 5600, Washington D.C. 20536-5600; sevp@ice.dhs.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Pub. L. No. 104-208, Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA); Pub. L. No. 106-215, Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA); Pub. L. No. 106-396, Visa Waiver Permanent Program Act of 2000

(VWPPA); Pub. L. No. 107-56, U.S.A. PATRIOT Act; Pub. L. No. 107-173, Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act); 8 C.F.R. § 214.2(f), (j), and (m); 8 C.F.R. §§ 214.3, 214.4, 214.5, 214.12, 214.13; 22 CFR Part 62; and Homeland Security Presidential Directive–2 (HSPD-2, Combating Terrorism Through Immigration Policies), as amended by HSPD–5, Management of Domestic Incidents (Feb. 28, 2003).

PURPOSE(S) OF THE SYSTEM: The purpose of this system of records is to maintain the integrity of the U.S. immigration system by collecting, maintaining, and analyzing information so that only bona fide nonimmigrant students or exchange visitors gain entry to the United States and that institutions accepting nonimmigrant students are legitimate and certified and adhere to the federal rules and regulations that govern them. DHS and DOS use of records covered by this system of records are for the following purposes:

Identity Validation – To identify and validate the identity of F/M/J nonimmigrants, federal government personnel, and school and program officials to ensure data integrity, accuracy, and proper data matching, as well as to authenticate individuals who either access SEVP systems or need to update information maintained by SEVP.

Determination and Status – To facilitate and support determination activities related to admissibility into the United States and the eligibility and status of benefits.

Adjudication – To 1) review and decide whether to certify a school or designate an EV Program so that F/M/J nonimmigrants may enroll or participate in the U.S.-based school or program; and 2) use supplemental information such as open-source media (e.g., publicly available information in newspaper articles, school websites, government websites, social media sites and blogs, online forums) to support vetting of F/M/J nonimmigrants and their dependents and school and program officials who handle personally identifiable information (PII) for other officials at their school or program.

Compliance – To monitor the compliance of F/M/J nonimmigrants, schools, programs, and school and program officials with immigration laws and regulations, including those addressing employment and training activities and immigration benefits, that govern the following: F and M nonimmigrants and the schools that enroll or seek to enroll them through the SEVP certification process; and participation of J nonimmigrants and programs within the EV Program.

Investigative – To perform administrative and criminal investigations related to the participation of F/M/J nonimmigrants, school and EV Program sponsors, and the schools and exchange visitor programs that enroll or seek to enroll individuals through the SEVP certification process, and to identify noncompliance with U.S. laws and regulations. Information is also shared with other law enforcement agencies for purposes of coordinating activities, such as administrative reviews and criminal investigations.

Analysis and Reporting – To create and provide reports for analyzing compliance issues and identifying activities and related individuals (if needed) for evidence-based decision-making.

Communication and Customer Relations – To provide customer service to individuals who contact the SEVP (e.g., via telephone, email, chat, social media), including providing general information about SEVP regulations, performing data corrections, and providing technical support to access SEVP systems.

Training – To keep track of training activities performed by school and program officials to validate compliance with SEVP requirements to access SEVP external-facing systems.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: SEVP collects, receives, captures, and maintains information on individuals who are U.S. citizens and lawful permanent residents, as well as information on persons who are currently nonimmigrants. DHS maintains this information in recognition that persons who are

nonimmigrants may later adjust status to lawful permanent resident and naturalize to U.S. citizen and, therefore, become individuals covered by the Privacy Act. DHS provides this notice in anticipation of such an eventuality :

F and M nonimmigrants who participate as students in an academic or vocational program at SEVP-certified schools, as well as F and M dependents (e.g., spouse, minor children).

J nonimmigrants who participate in DOS-designated work or study exchange visitor programs, as well as J dependents (e.g., spouse, minor children).

Proxy, parent, or legal guardian who has legal authority to make decisions or sign documents on behalf of another individual who participates in a student and exchange visitor program (e.g., a minor, an individual with disabilities).

School partners and representatives including the head of school (e.g., owner, president, chief executive officer [CEO], legal counsel) who has legal signature authority for the school and school employees (e.g., faculty members, student recruiters) who are employed by a U.S.-based school and interact with F and M students but who do not oversee the F and M students pursuant to the laws and regulations governing F and M nonimmigrant students and schools that enroll them (this is the responsibility of school officials). Also included are school partners (e.g., contractor who builds housing facility, sports program that uses school space) who provide a service for a school or manage activities on school sites that impact F and M students but who are not employees of the school.

School officials (individuals who are U.S. citizens or lawful permanent residents) who submit information for school SEVP certification and recertification and oversee F and M students enrolled at their school.

Exchange visitor program sponsors (e.g., an entity seeking to sponsor a nonimmigrant au pair, research scholar, intern, or government visitor) who must be

designated by DOS to run an EV Program and host J nonimmigrants. This includes the program sponsor (e.g., owner, CEO, legal counsel) who has legal signature authority for the EV Program sponsor.

Program officials (individuals who are U.S. citizens or lawful permanent residents) who submit information for EV Program sponsor DOS designation and re-designation and oversee J nonimmigrants enrolled in programs offered by the sponsor.

Host families (individuals who are U.S. citizens or lawful permanent residents) who provide living arrangements for J nonimmigrants.

Financial support provider who, as an individual, organization, or government, provides support to F/M/J nonimmigrants.

Employers (e.g., supervisor, official with signature authority) of F/M/J nonimmigrants with authority to work in the United States.

Federal government personnel (i.e., federal employees and contractors) who manage the SEVP program and use information maintained by SEVP to support the DHS mission, and coordinate with DOS with respect to the J exchange visitor program-related data. Federal government personnel also use SEVP information to support other federal agency missions that align with DHS's and DOS's oversight of nonimmigrant students and exchange visitors, including the ED, Department of Commerce, Department of Justice – Federal Bureau of Investigation, and federal intelligence agencies.

State government personnel (i.e., state employees and contractors) who interact with federal government personnel and exchange information for activities related to administrative reviews and investigations.

Governing bodies (e.g., licensing and accrediting bodies) that ensure the education provided by schools meets acceptable levels of quality and grant licenses and accreditation to schools that meet these criteria.

Members of the public (e.g., property owners, holding companies, school officials, F and M nonimmigrants, individuals of the general population) who (1) provide SEVP with information about things such as a school, program, or individual aligned with SEVP and potential infractions or illegal activities; (2) provide feedback about SEVP on the performance of SEVP employees, its programs, or its regulations; or (3) contact SEVP for other reasons.

CATEGORIES OF RECORDS IN THE SYSTEM: The various categories of information (including PII and sensitive PII) collected, received, captured, used, shared, and maintained by SEVP and DOS on the individuals identified above are as follows:

Biographical – Includes full name; gender; date of birth; country of birth; country of citizenship; country of legal permanent residence; contact information (e.g., telephone number, email address, physical/mailling address); and full name and contact information of proxy, parent, or legal guardian for F/M/J nonimmigrant.

Criminal History – Includes arrest and bail information, case number, date charges were filed, case type, initial criminal offense type, date of crime, disposition and judgment date, and county jurisdiction.

Identity Verification – Includes identity documents (e.g., driver's license, passport); unique identifiers (e.g., SEVIS ID, immigration identification number [IIN], official personal identification number [OPID], A-number, passport number, limited instances of incidental collection of social security number); and biometric identifiers (e.g., fingerprint identification number [FIN]).

Education – Includes education transcripts; certificates of graduation; program of study (e.g., types of program, courses, level of education); length of study; school registration information; school admission number; school transfer information; extensions; and changes to program of study or activity.

Exchange visitor program – Includes exchange visitor program information (e.g., type of program, program activities); placement information (e.g., site of activity, host family, host family contact information, EV Program sponsor name); extensions; and changes to program or activity.

Employment – Includes practical training information (e.g., training plan); employer and supervisor information (e.g., name of employer, name of supervisor); employer and supervisor contact information (e.g., telephone number, email address, website URL); employer identification number; and employment information (e.g., position title, description of duties, employment authorization document number).

Financial – Includes financial support information (e.g., sources of funding); payment receipt information related to school certification and EV Program sponsor designation fees; and payment receipt information for the Form I-901 fee.

Travel – Includes visa information (e.g., visa number, country of issuance, expiration date); passport information (e.g., passport number, expiration date, country issued); and arrival and departure information.

Immigration-Related – Includes entry into and exit from the United States (e.g., Form I-94 admission number, dates of entry and exit, ports of entry); class of admission (e.g., visa type); immigration status; adjudication decisions; and, immigration benefit application information (e.g., adjustment of status).

School – Includes school name; contact information (e.g., telephone number, email address, physical mailing address); open-source media information (e.g., publicly available information available in newspaper articles, websites, personal and organizational social media); school's program information (e.g., site locations, addresses, phone number, school code); school's accreditation and certification information and documentation; and documented evidence from nonaccredited schools (e.g., articulation agreements, state-issued professional licenses).

Program Sponsor – Includes program sponsor name; CEO name and contact information (e.g., telephone number, email address, physical mailing address); and, location and contact information (e.g., site locations, addresses, phone number).

Case-Related – Includes case number; adjudication determinations; site visit reports; appeals determinations; administrative reviews; and information regarding investigations.

Auditing and Training – Includes auditing information (e.g., IP addresses, access and change history, date/time access, username, user role); system login (e.g., username, password, email address, name of individual); unique identifier (e.g., SEVIS ID, IIN, OPID); and training information (e.g., training status, training certificates, training transcripts).

Reporting – Includes reporting information (e.g., aggregate data, statistics on overstays).

Inquiries and Data Corrections – Includes contact information (e.g., telephone number, email address, physical mailing address); unique identifier (e.g., SEVIS ID, IIN, OPID); identity documents (e.g., driver's license, passport, marriage certificate); and information not previously collected (e.g., new address, passport number) by SEVP to facilitate handling inquiries and data corrections.

RECORD SOURCE CATEGORIES: Records are obtained from F/M/J nonimmigrants; proxy, parent, or legal guardians; school officials; program officials; federal and state government personnel; federal agency systems; governing bodies; and members of the public.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a

portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorney's Offices, or other federal agencies conducting litigation or proceedings before any court, adjudicative, or administrative body, when it is relevant and necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee or former employee of DHS in his or her official capacity;
3. Any employee or former employee of DHS in his or her individual capacity, only when DOJ or DHS has agreed to represent the employee;
4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the federal government, or national security; and (3) the disclosure made to such agencies, entities,

and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another federal agency or federal entity when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the federal government, or national security resulting from a suspected or confirmed breach.

G. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

H. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

I. For investigative material compiled for law enforcement purposes, to appropriate federal, state, tribal, local, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws.

J. To a court, magistrate, administrative tribunal, opposing counsel, parties, and witnesses in the course of a civil, criminal or administrative proceeding before a court or adjudicative body when DHS determines that the use of such records is relevant and necessary to the litigation or the proceeding and one of the following is a party to, or has an interest in, the litigation or the proceeding:

1. DHS or any component thereof;
2. Any employee of DHS in his or her official capacity;
3. Any employee of DHS in his or her individual capacity where the agency has agreed to represent the employee;
4. The United States, where DHS determines that litigation is likely to affect DHS or any of its components.

K. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings.

L. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats. Appropriate notice of any identified health threat or risk will be given.

M. To foreign governments for the purpose of providing information about their citizens or permanent residents, or family members thereof, during a school closing, local or national disasters, or health emergencies.

N. To the U.S. Treasury Department and its contractors to facilitate and track SEVP fee payments made by F/M/J nonimmigrants.

O. To schools and exchange visitor sponsors participating in the SEVP or EV Program for the purpose of certification and designation, enrollment, transfer, and monitoring of F/M/J nonimmigrants, audit, oversight, and compliance enforcement.

P. To the DOS for the purpose of visa issuance to F/M/J nonimmigrants; the operation of its exchange visitor program; or the enforcement of, and investigation into, its visa and exchange visitor program laws, regulations, and requirements.

Q. To the DOS in the processing of petitions or applications for benefits under the Immigration and Nationality Act and all other immigration and nationality laws including treaties and reciprocal agreements.

R. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data that relate to the purposes stated in this SORN in order to test, develop, and implement new technologies for the purposes of data sharing to support and enhance the efficiency of the SEVP or homeland security.

S. To a federal, state, tribal, local, international, or foreign government agency or entity for the purpose of consulting with that agency or entity:

1. To assist in making a determination about redress provided under the Privacy Act for an individual in connection with the operations of a DHS component or program.
2. For the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS component or program.
3. For the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

T. To a former employee of DHS for purposes of (1) responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable DHS regulations; or (2) facilitating communications with a

former employee that may be necessary for personnel-related or other official purposes when DHS requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

U. To a federal state, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

V. To an accrediting agency, recognized by ED, for the purpose of performing accreditation activities for schools and exchange visitor programs, including accreditation of English-language training programs in accordance with the Accreditation of English Language Training Programs Act (Pub. L. 111-306), but only such as is necessary and relevant to such accreditation function.

W. To an appropriate Federal, State, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request.

X. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there is a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the

CPO determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS/ICE stores records in these systems electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by biographical and unique verification identifiers such as full name, date of birth, email address, SEVIS ID, IIN, FIN, OPID, and A-number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF

RECORDS: An SEVP program-wide, media-neutral records retention schedule is currently under development. ICE is proposing a 75-year retention schedule for program-specific records maintained by SEVP to facilitate program operations and carry out the mission objectives of the Agency. ICE will maintain these records permanently, until an Agency retention schedule is submitted to the National Archives and Records Administration (NARA) and approved by the Archivist of the United States. All other federal Agency records will be maintained in accordance with the appropriate general records schedule (GRS). For example, ICE will follow the appropriate retention periods outlined in the NARA-approved GRS for administrative records (e.g., audit information, system login, inquiries, reporting). The NARA-approved GRS can be found at <https://www.archives.gov/records-mgmt/grs>.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/ICE safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS/ICE has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those

who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: The Secretary of Homeland Security has exempted this system of records from the notification, access, and amendment procedures of the Privacy Act, and the JRA if applicable, because it is a law enforcement system of records. However, DHS/ICE will consider individual requests to determine whether information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the ICE Privacy Officer and ICE Freedom of Information Act (FOIA) Officer, whose contact information can be found at <https://www.dhs.gov/foia> under “Contact Information.” If an individual believes more than one component maintains his or her Privacy Act records, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the JRA provides a right of access, certain records about an individual may be available under the FOIA.

When an individual is seeking his or her records about from this system of records or any other departmental system of records, the individual’s request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his or her identity, meaning that the individual must provide full name, current address, and date and place of birth. The individual must sign the request, and the signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. Although no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, <https://www.dhs.gov/foia>, or call (866) 431-0486. In addition, you should do the following:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believe may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If an individual's request is seeking records pertaining to another living individual, the first individual must include a statement from the second individual certifying that individual's agreement for the first individual to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, individuals may make a request for amendment or correction of a record by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

To correct an ICE record, individuals may submit a Privacy Act amendment request by completing DHS Form 500-05 "Certification of Identity," which can be found at <https://www.ice.gov/privacy>. The signed form and a detailed request should be sent to

the ICE Office of Information Governance and Privacy at ICEPrivacy@ice.dhs.gov, or to the following address:

U.S. Immigration and Customs Enforcement

ICE Information Governance and Privacy

ATTN: Privacy Office

500 12th Street SW, Stop 5004

Washington, D.C. 20536-5004

NOTIFICATION PROCEDURES: See the “Record Access Procedures” section.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. secs. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g)(1). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a (k)(1) and (k)(2), has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. secs. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).

When this system receives a record from another system exempted in that source system under 5 U.S.C. sec. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary system of records from which they originated and claims any additional exemptions set forth here.

HISTORY: 75 Fed. Reg. 412 (Jan. 5, 2010); 73 Fed. Reg. 63057 (Oct. 23, 2008).

Lynn Parker Dupree,

Chief Privacy Officer,

U.S. Department of Homeland Security.

[FR Doc. 2021-26477 Filed: 12/7/2021 8:45 am; Publication Date: 12/8/2021]